适用于 ACI 的 Cisco ASA Device Package 软件的 XML 示例

Revised: 2020 年 12 月 28 日

XML 示例

简介

本文档提供通过应用策略基础设施控制器 (APIC) 北向 API 支持的 ASA 功能的 XML 示例。不过，本文档不包括适用于这些服务的所有 ASA 功能选项的完整列表。要确定北向 API 允许的选项，您应使用随 ASA 设备包提供的 *device_specification.xml* 文件。

有关如何使用 APIC 北向 API 的信息，请参阅《思科 APIC 管理信息模型参考》。

可用的 APIC 产品

从 1.2(7.8) 开始，适用于 ACI 的 Cisco ASA Device Package 软件有两个版本：

- 思科 ASA 设备包 - 插入阵列的策略协调。您可以通过此版本从 APIC 配置 ASA 的许多重要功能，包括（但不限于）以下内容：
  - 接口
  - 路由
  - Access-list
  - NAT
  - TrustSec
  - 应用检测
  - NetFlow
  - 高可用性
  - 站点到站点 VPN
- 思科 ASA 设备包 - 插入阵列。此版本包含原始版本的以下功能：
  - 接口
  - 动态路由
  - 静态路由

北向 API

以下是访问 ASA 的示例 XML。对于多情景 ASA，直接在 vnsLDevVip 下的访问信息是 ASA 中的管理情景；vnsCDev 文件夹中的访问信息是目标用户情景。同样，管理情景也可用作目标用户情景。

此处只允许来自给定多情景 ASA 的一个情景。

```
<polUni>
<fvTenant
dn="uni/tn-tenant1"
name="tenant1">
<vnsLDevVip name="Firewall" devtype="PHYSICAL">
<vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.2"/>
<!---Admin context access information ---/>
<vnsCMgmt name="devMgmt" host="172.23.204.205" port="443"/>
<vnsCCred name="username" value="admin"/>
<vnsCCredSecret name="password" value="somepassword"/>

<vnsCDev name="ASA">
<!---User context access information ---/>
<vnsCMgmt name="devMgmt" host="172.23.204.123" port="443" />
<vnsCCred name="username" value="admin" />
<vnsCCredSecret name="password" value="otherpassword" />
</vnsCDev>
</vnsLDevVip>

</fvTenant>
</polUni>
```

接口

接口通常设置为 APIC 上总体基础设施中使用服务图的一部分。图形与合同、具体设备、逻辑设备和逻辑接口关联。图形还需要接口 IP 地址在先前为关联租户定义的适当范围内。图形设置显示各种接口类型。对于 ASAv，接口在 ASA 本身上使用物理接口定义。对于硬件 ASA，接口使用 VlAN 定义。定义接口的 XML 文件相同，设备包使用“devtype”字段（“PHYSICAL”或“VIRTUAL”）以确定要发送到 ASA 进行配置的正确 CLI。“FuncType”字段（“GoTo”或“GoThrough”）确定接口是用于透明防火墙还是路由防火墙。

透明网桥组虚拟接口

此 XML 示例创建以下网桥组并添加网桥组成员。此示例针对硬件 ASA；VLAN 为动态分配。

ASA 配置

```
interface GigabitEthernet0/0
no nameif
no security-level

interface GigabitEthernet0/0.987
vlan 987
nameif externalIf
bridge-group 1
security-level 50

interface GigabitEthernet0/1
no nameif
no security-level

interface GigabitEthernet0/1.986
vlan 986
nameif internalIf
bridge-group 1
security-level 100
```

```
interface BVI1
ip address 10.10.10.2 255.255.255.0
```

XML 示例

定义图形和接口，然后将其附加到租户。

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsTermNodeCon name = "Input1">
<vnsAbsTermConn name = "C1"/>
</vnsAbsTermNodeCon>
<!-- FW1 Provides FW functionality -->
<vnsAbsNode name = "FW1" funcType="GoThrough">
<vnsRsDefaultScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

<vnsAbsFuncConn name = "external" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external" />
</vnsAbsFuncConn>
<vnsAbsFuncConn name = "internal" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal" />
</vnsAbsFuncConn>
<vnsAbsDevCfg>
<vnsAbsFolder key="BridgeGroupIntf" name="1">
<vnsAbsFolder key="IPv4Address" name="internalIfIP">
<vnsAbsParam key="ipv4_address" name="ipv4" value="10.10.10.2/255.255.255.0"/>
<vnsAbsParam key="ipv4_standby_address" name="ipv4s" value="10.10.10.3"/>
</vnsAbsFolder>
</vnsAbsFolder>

<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
<vnsAbsCfgRel key="bridge_group" name="intbridge" targetName="1"/>
<vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
<vnsAbsCfgRel key="bridge_group" name="extbridge" targetName="1"/>
<vnsAbsParam key="security_level" name="external_security_level" value="50"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>

<vnsAbsFuncCfg>
<vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfigA">
<vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
</vnsAbsFolder>

<vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfigA">
<vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
</vnsAbsFolder>
</vnsAbsFuncCfg>

<vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
</vnsAbsNode>
```

```
<vnsAbsTermNodeProv name = "Output1">
<vnsAbsTermConn name = "C6"/>
</vnsAbsTermNodeProv>
<vnsAbsConnection name = "CON1">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn"/>
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external"/>
</vnsAbsConnection>
<vnsAbsConnection name = "CON2" unicastRoute="no">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal"/>
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn"/>
</vnsAbsConnection>
</vnsAbsGraph>

</fvTenant>
</polUni>
```

路由防火墙接口

此 XML 示例创建以下路由接口。此示例针对硬件 ASA；VLAN 为动态分配。

ASA 配置

```
interface GigabitEthernet0/0.655
vlan 655
mac-address 00aa.00bb.00cc standby 00ff.00ff.ffff
nameif externalIf
security-level 50
ip address 20.20.20.20 255.255.255.0 standby 20.20.20.21

interface GigabitEthernet0/1.968
vlan 968
nameif internalIf
security-level 100
ip address 10.10.10.10 255.255.255.0 standby 10.10.10.11
```

XML 示例

定义图形，然后将其附加到租户。

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">

<vnsAbsTermNodeCon name = "Input1">
<vnsAbsTermConn name = "C1">
</vnsAbsTermConn>
</vnsAbsTermNodeCon>

<!-- FW1 Provides FW functionality -->
<vnsAbsNode name = "FW1">
<vnsRsDefaultScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

<vnsAbsFuncConn name = "external" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external" />
</vnsAbsFuncConn>

<vnsAbsFuncConn name = "internal" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal" />
</vnsAbsFuncConn>
<vnsAbsDevCfg>
```

```
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
<vnsAbsFolder key="IPv4Address" name="internalIfIP">
<vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
<vnsAbsParam key="ipv4_standby_address" name="ipv4_internals" value="10.10.10.11"/>
</vnsAbsFolder>
<vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
<vnsAbsFolder key="IPv4Address" name="externalIfIP">
<vnsAbsParam key="ipv4_address" name="ipv4_external" value="20.20.20.20/255.255.255.0"/>
<vnsAbsParam key="ipv4_standby_address" name="ipv4_externals" value="20.20.20.21"/>
</vnsAbsFolder>
<vnsAbsParam key="security_level" name="external_security_level" value="50"/>
<vnsAbsFolder key="mac_address" name="mac">
<vnsAbsParam key="active_mac" name="activemac" value="aa.bb.cc"/>
<vnsAbsParam key="standby_mac" name="stbymac" value="ff.ff.ffff"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>

<vnsAbsFuncCfg>
<vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfig">
<vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
</vnsAbsFolder>

<vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfig">
<vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
</vnsAbsFolder>

</vnsAbsFuncCfg>

<vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
</vnsAbsNode>

<vnsAbsTermNodeProv name = "Output1">
<vnsAbsTermConn name = "C6">
</vnsAbsTermConn>
</vnsAbsTermNodeProv>
<vnsAbsConnection name = "CON1">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn" />
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
</vnsAbsConnection>
<vnsAbsConnection name = "CON2">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn" />
</vnsAbsConnection>

</vnsAbsGraph>
<vzBrCP name="webCtrct">
<vzSubj name="http">
<vzRsSubjGraphAtt tnVnsAbsGraphName="WebGraph"/>
</vzSubj>
</vzBrCP>
</fvTenant>
</polUni>
```

端口通道接口

此 XML 示例创建以下端口通道成员和端口通道接口（此时仅在物理 ASA 上受支持）。

ASA 配置

```
interface GigabitEthernet0/0
channel-group 2 mode active
no nameif
no security-level
no ip address

interface GigabitEthernet0/1
channel-group 1 mode active
no nameif
no security-level
no ip address

interface Port-channel1.100
vlan 100
nameif externalIf
security-level 50
ip address 20.20.20.20 255.255.255.0 standby 20.20.20.21

interface Port-channel2.200
vlan 200
nameif internalIf
ip address 10.10.10.10 255.255.255.0 standby 10.10.10.11
```

XML 示例

定义端口通道成员、图形，然后将其附加到租户。

```
<polUni>
<fvTenant dn="uni/tn-tenant1" name="tenant1">
<vnsLDevVip name="Firewall" funcType="GoTo" devtype="PHYSICAL">
<vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}"/>
<vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
<vnsCMgmt name="devMgmt" host="10.122.202.33" port="443" />
<vnsCCred name="username" value="management-user"/>
<vnsCCredSecret name="password" value="cisco"/>
<vnsDevFolder key="PortChannelMember" name="PC1a">
<vnsDevParam key="port_channel_id" name="PC1a" value="1"/>
<vnsDevParam key="interface" name="PC1a" value="Gig0/1"/>
</vnsDevFolder>
<vnsDevFolder key="PortChannelMember" name="PC2a">
<vnsDevParam key="port_channel_id" name="PC2a" value="2"/>
<vnsDevParam key="interface" name="PC2a" value="Gig0/0"/>
</vnsDevFolder>
</vnsLDevVip>
<vnsLDevCtx ctrctNameOrLbl="webCtrct" graphNameOrLbl="WebGraph" nodeNameOrLbl="FW1">
<vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevVip-Firewall"/>
<vnsLIfCtx connNameOrLbl="internal">
<vnsRsLIfCtxToBD tDn= "uni/tn-tenant1/BD-tenant1BD1"/>
<vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-internalPC"/>
</vnsLIfCtx>
<vnsLIfCtx connNameOrLbl="external">
<vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-externalPC"/>
<vnsRsLIfCtxToBD tDn= "uni/tn-tenant1/BD-tenant1BD2"/>
```

```
</vnsLIfCtx>
</vnsLDevCtx>
</fvTenant>
</polUni>

<polUni>
<fvTenant name="tenant1">

<vnsAbsGraph name = "WebGraph">

<vnsAbsTermNodeCon name = "Input1">
<vnsAbsTermConn name = "C1">
</vnsAbsTermConn>
</vnsAbsTermNodeCon>

<!-- FW1 Provides FW functionality -->
<vnsAbsNode name = "FW1">
<vnsRsDefaultScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

<vnsAbsFuncConn name = "external" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external" />
</vnsAbsFuncConn>

<vnsAbsFuncConn name = "internal" attNotify="yes">
<vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal" />
</vnsAbsFuncConn>
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
<vnsAbsFolder key="IPv4Address" name="internalIfIP">
<vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
<vnsAbsParam key="ipv4_standby_address" name="ipv4_internals" value="10.10.10.11"/>
</vnsAbsFolder>
<vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
</vnsAbsFolder>

</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
<vnsAbsFolder key="IPv4Address" name="externalIfIP">
<vnsAbsParam key="ipv4_address" name="ipv4_external" value="20.20.20.20/255.255.255.0"/>
<vnsAbsParam key="ipv4_standby_address" name="ipv4_externals" value="20.20.20.21"/>
</vnsAbsFolder>
<vnsAbsParam key="security_level" name="external_security_level" value="50"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>

<vnsAbsFuncCfg>
<vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfig">
<vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
</vnsAbsFolder>

<vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfig">
<vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
<vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
<vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
</vnsAbsFolder>

</vnsAbsFuncCfg>

<vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
```

```
</vnsAbsNode>

<vnsAbsTermNodeProv name = "Output1">
<vnsAbsTermConn name = "C6">
</vnsAbsTermConn>
</vnsAbsTermNodeProv>
<vnsAbsConnection name = "CON1">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn" />
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
</vnsAbsConnection>
<vnsAbsConnection name = "CON2">
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
<vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn" />
</vnsAbsConnection>

</vnsAbsGraph>
</fvTenant>
</polUni>

<polUni>
<fvTenant name="tenant1">
<vzBrCP name="webCtrct">
<vzSubj name="http">
<vzRsSubjGraphAtt tnVnsAbsGraphName="WebGraph"/>
</vzSubj>
</vzBrCP>
</fvTenant>
</polUni>
```

访问列表和关联访问组

此 XML 示例创建访问列表，并将其分配到与现有接口关联的访问组。

ASA 配置

```
access-list ACL2 extended deny ip any any
access-list ACL2 extended permit icmp any any
access-list ACL1 extended permit tcp any any eq ssh
access-list ACL1 extended permit tcp any any eq https

access-group ACL2 in interface externalIf
access-group ACL1 out interface internalIf
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="ACL1">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
<vnsAbsFolder key="protocol" name="protocol1">
<vnsAbsParam key="name_number" name="pNN1" value="tcp"/>
</vnsAbsFolder>
<vnsAbsFolder key="destination_service" name="d1">
<vnsAbsParam key="operator" name="dop1" value="eq"/>
```

```
<vnsAbsParam key="low_port" name="dlp1" value="ssh"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="AccessControlEntry" name="ACE2">
<vnsAbsParam key="action" name="action2" value="permit"/>
<vnsAbsParam key="order" name="order2" value="2"/>
<vnsAbsFolder key="protocol" name="protocol2">
<vnsAbsParam key="name_number" name="pNN2" value="tcp"/>
</vnsAbsFolder>
<vnsAbsFolder key="destination_service" name="d2">
<vnsAbsParam key="operator" name="dop2" value="eq"/>
<vnsAbsParam key="low_port" name="dlp2" value="https"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="AccessList" name="ACL2">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="deny"/>
<vnsAbsParam key="order" name="order1" value="1"/>
</vnsAbsFolder>
<vnsAbsFolder key="AccessControlEntry" name="ACE2">
<vnsAbsParam key="action" name="action2" value="permit"/>
<vnsAbsParam key="order" name="order2" value="2"/>
<vnsAbsFolder key="protocol" name="protocol2">
<vnsAbsParam key="name_number" name="pNN2" value="icmp"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder name="IntAccessGroup" key="AccessGroup">
<vnsAbsCfgRel key="outbound_access_list_name" name="iACG" targetName="ACL1"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder name="ExtAccessGroup" key="AccessGroup">
<vnsAbsCfgRel key="inbound_access_list_name" name="oACG" targetName="ACL2"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

使用动态创建的 EPG 网络对象的访问列表

此 XML 示例创建动态更新 ACL 中对象组成员的访问列表，其中对象组与端点组 (EPG) 相对应。

注释 您必须在 APIC 中创建必需的 *AccessControlEntry*。

ASA 配置

```
access-list EPG_ACL extended permit ip object-group __$EPG$_web object-group __$EPG$_app
access-group EPG_ACL in interface externalIf
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="EPG_ACL">
<vnsAbsFolder key="AccessControlEntry" name="EPG_ACE">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
<vnsAbsFolder key="source_address" name="saddr1">
<vnsAbsParam key="epg_name" name="webEPG" value="tenantname-profilename-web"/>
</vnsAbsFolder>
<vnsAbsFolder key="destination_address" name="daddr1">
<vnsAbsParam key="epg_name" name="appEPG" value="tenantname-profilename-app"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder name="access-group-EPG" key="AccessGroup">
<vnsAbsCfgRel name="name" key="inbound_access_list_name" targetName="EPG_ACL"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

IP 审核

此 XML 示例设置 IP 审核攻击配置。

ASA 配置

```
ip audit attack action drop
```

XML 示例（攻击）

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="IPAudit" name="A">
<vnsDevParam key="IPAuditAttack" name="IPattack" value="drop"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

此 XML 示例还设置 IP 审核攻击配置。

ASA 配置

```
ip audit attack action reset
```

XML 示例（信息）

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="IPAudit" name="A">
<vnsDevParam key="IPAuditInfo" name="IPinfo" value="reset"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

日志记录

此 XML 示例设置日志记录配置。

ASA 配置

```
logging enable
logging buffer-size 8192
logging buffered critical
logging trap alerts
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="LoggingConfig" name="Log">
<vnsDevParam key="enable_logging" name="enlog" value="enable"/>
<vnsDevParam key="buffered_level" name="bufflev" value="critical"/>
<vnsDevParam key="buffer_size" name="buffsize" value="8192"/>
<vnsDevParam key="trap_level" name="trap" value="1"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

Static Route

此 XML 示例设置与现有接口关联的静态路由配置。

ASA 配置

```
route internalIf 10.100.0.0 255.255.0.0 10.6.55.1 1
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
```

```
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="StaticRoute" name="InsideRTE1">
<vnsAbsFolder key="route" name="RouteIN1">
<vnsAbsParam key="network" name="network1" value="10.100.0.0"/>
<vnsAbsParam key="netmask" name="netmask1" value="255.255.0.0"/>
<vnsAbsParam key="gateway" name="gateway1" value="10.6.55.1"/>
<vnsAbsParam key="metric" name="metric1" value="1"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

基本威胁检测

此 XML 示例设置 ACL 丢弃的基本威胁检测率。

ASA 配置

```
threat-detection rate acl-drop rate-interval 600 average-rate 0 burst-rate 0
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="BasicThreatDetection" name="BasicTD">
<vnsDevParam key="basic_threat" name="Basic1" value="enable"/>
<vnsDevFolder key="BasicThreatDetectionRateAclDrop" name="BasicTDACL">
<vnsDevParam key="rate_interval" name="ri1" value="600"/>
<vnsDevParam key="average_rate" name="ar1" value="0"/>
<vnsDevParam key="burst_rate" name="br1" value="0"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

扫描威胁检测

此 XML 示例设置扫描威胁检测率。

ASA 配置

```
threat-detection rate scanning-threat rate-interval 600 average-rate 100 burst-rate 40
threat-detection scanning-threat shun
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="ScanningThreatDetection" name="ScanTD1">
<vnsDevParam key="scanning_threat" name="Scan1" value="enable"/>
<vnsDevParam key="shun_status" name="Shun1" value="enable"/>
<vnsDevFolder key="ScanningThreatRate" name="ScanTDrate">
<vnsDevParam key="average_rate" name="ar1" value="100"/>
<vnsDevParam key="rate_interval" name="ri1" value="600"/>
<vnsDevParam key="burst_rate" name="br1" value="40"/>
</vnsDevFolder>
<vnsDevFolder key="ScanningThreatRate" name="ScanTDrate2">
<vnsDevParam key="average_rate" name="ar2" value="10"/>
<vnsDevParam key="rate_interval" name="ri2" value="660"/>
<vnsDevParam key="burst_rate" name="br2" value="20"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

高级威胁检测

此 XML 示例设置高级威胁检测统计信息。

ASA 配置

```
threat-detection statistics host
threat-detection statistics port number-of-rate 2
threat-detection statistics protocol number-of-rate 3
threat-detection statistics tcp-intercept rate-interval 50 burst-rate 200 average-rate 100
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="AdvancedThreatDetection" name="AdvScan" >
<vnsDevParam key="access_list" name="status5" value="enable"/>
<vnsDevFolder key="AdvancedThreatDetectionTcpIntercept" name="AdvScanTCPInt" >
<vnsDevParam key="status" name="AdvRateStatus" value="enable"/>
<vnsDevParam key="average_rate" name="AdvRate" value="100"/>
<vnsDevParam key="rate_interval" name="AdvRI" value="50"/>
<vnsDevParam key="burst_rate" name="AdvBR" value="200"/>
</vnsDevFolder>
<vnsDevFolder key="AdvancedThreatDetectionHost" name="AdvScanHost" >
<vnsDevParam key="status" name="HostStatus" value="enable"/>
<vnsDevParam key="number_of_rate" name="HostRate" value="1"/>
</vnsDevFolder>
<vnsDevFolder key="AdvancedThreatDetectionPort" name="AdvScanPort" >
<vnsDevParam key="status" name="PortStatus" value="enable"/>
<vnsDevParam key="number_of_rate" name="PortRate" value="2"/>
</vnsDevFolder>
<vnsDevFolder key="AdvancedThreatDetectionProtocol" name="AdvScanProtocol" >
<vnsDevParam key="status" name="ProtocolStatus" value="enable"/>
<vnsDevParam key="number_of_rate" name="ProtocolRate" value="3"/>
```

```
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

协议超时

此 XML 示例设置连接计时器的协议超时值。

ASA 配置

```
timeout conn 2:00:59
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="Timeouts" name="TO">
<vnsDevParam key="Connection" name="conn1" value="2:0:59"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

网络时间协议

此 XML 示例启用网络时间协议 (NTP) 功能以定义要使用的服务器。

ASA 配置

```
ntp server 192.168.100.100 prefer
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="NTP" name="NTP">
<vnsDevFolder key="NTPServer" name="NTPServer">
<vnsDevParam key="server" name="server" value="192.168.100.100"/>
<vnsDevParam key="prefer" name="prefer" value="enable"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

Smart Call-Home

此 XML 示例启用带有匿名报告的 Smart Call-Home 功能。

ASA 配置

```
call-home reporting anonymous
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="SmartCallHome" name="SmartCallHome">
<vnsDevParam key="anonymous_reporting" name="anonymous_reporting" value="enable"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

域名系统

此 XML 示例启用域名系统 (DNS) 功能，将其链接到实用程序接口，并指定要使用的域名和服务器 IP 地址。

ASA 配置

注释　您必须使用 **nameif management-utility** 命令在 ASA 上预先配置实用程序接口。

```
dns domain-lookup management-utility
dns server-group DefaultDNS
name-server 1.1.1.1
domain-name testDomain
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="DNS" name="DNS">
<vnsDevParam key="domain_name" name="domain_name" value="testDomain"/>
<vnsDevParam key="name_server" name="name_server" value="1.1.1.1"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

连接限制

此 XML 示例显示与接口关联的连接限制（不支持全局连接限制）、匹配任何流量，并设置允许的最大连接数。此外还包括内部和外部接口上的连接限制。

ASA 配置

```
class-map connlimits_internalIf
match any

policy-map internalIf
class connlimits_internalIf
set connection conn-max 654 embryonic-conn-max 456

service-policy internalIf interface internalIf
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="ServicePolicy" name="ConLim-Policy">
<vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
<vnsAbsFolder key="ConnectionLimits" name="ConnLim">
<vnsAbsFolder key="ConnectionSettings" name="ConnectionSettingsA">
<vnsAbsParam key="conn_max" name="conn_max" value="654"/>
<vnsAbsParam key="conn_max_embryonic" name="conn_max_embryonic" value="456"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

应用检测

此 XML 示例显示与接口关联的应用检测（不支持全局应用检测）、匹配默认检测流量，并启用 HTTP 检测。此外还包括内部和外部接口上的应用检测。

ASA 配置

```
class-map inspection_internalIf
match default-inspection-traffic

policy-map internalIf
class inspection_internalIf
inspect http
```

```
service-policy internalIf interface internalIf
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="ServicePolicy" name="Inspection-Policy">
<vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
<vnsAbsFolder key="ApplicationInspection" name="ApplicationInspection">
<vnsAbsFolder key="InspectionSettings" name="InspectionSettingsA">
<vnsAbsParam key="http" name="http" value="enable"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

全局 NetFlow

此 XML 示例设置 NetFlow 功能。此示例显示如何创建与流量匹配的简单访问列表、创建 NetFlow 对象并为 NetFlow 对象全局启用 NetFlow。此外还包括内部和外部接口上的 NetFlow。

ASA 配置

```
class-map netflow_default
match any

flow-export destination management-utility 1.2.3.4 1024
flow-export template timeout-rate 120
flow-export delay flow-create 60
flow-export active refresh-interval 30

class netflow_default
flow-export event-type all destination 1.2.3.4
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="NetFlowObjects" name="ObjectA">
<vnsDevFolder key="TemplateAndCollectors" name="TemplateA">
<vnsDevParam key="template_timeout_rate" name="timeout" value="120"/>
<vnsDevParam key="delay_flow_create" name="delay" value="60"/>
<vnsDevParam key="active_refresh_interval" name="refresh" value="30"/>
<vnsDevFolder key="NetFlowCollectors" name="CollectorA">
<vnsDevParam key="status" name="status" value="enable"/>
<vnsDevParam key="host" name="host" value="1.2.3.4"/>
```

```
<vnsDevParam key="port" name="port" value="1024"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
<vnsDevFolder key="GlobalServicePolicy" name="GlobalPolicyA">
<vnsDevParam key="ServicePolicyState" name="PolicyState" value="enable"/>
<vnsDevFolder key="NetFlow" name="NetFlowPolicyA">
<vnsDevFolder key="NetFlowSettings" name="SettingA">
<vnsDevFolder key="ExportAllEvent" name="ExportAll">
<vnsDevParam key="status" name="status" value="enable"/>
<vnsDevParam key="event_destination" name="dest" value="1.2.3.4"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

网络地址转换

此 XML 示例基于先前创建的网络对象（ilinux1 和 olinux1）在外部接口上设置网络地址转换 (NAT) 功能。

ASA 配置

```
nat (externalIf,internalIf) source static ilinux1 olinux1
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="NATList" name="ListA">
<vnsAbsFolder key="NATRule" name="RuleA">
<vnsAbsParam key="order" name="order" value="3"/>
<vnsAbsFolder key="source_translation" name="source_trans">
<vnsAbsFolder key="mapped_object" name="mapped_object">
<vnsAbsCfgRel key="object_name" name="map_name" targetName="olinux1"/>
</vnsAbsFolder>
<vnsAbsFolder key="real_object" name="real_object">
<vnsAbsCfgRel key="object_name" name="real_name" targetName="ilinux1"/>
</vnsAbsFolder>
<vnsAbsParam key="nat_type" name="nat_type" value="static"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
<vnsAbsFuncCfg>
<vnsAbsFolder key="NATPolicy" name="PolicyA">
<vnsAbsCfgRel key="nat_list_name" name="nat_listA" targetName="ListA"/>
</vnsAbsFolder>
</vnsAbsFuncCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
```

```
</polUni>
```

入侵防御系统

此 XML 示例设置入侵防御系统 (IPS) 功能。此示例显示如何匹配流量与先前创建的访问列表 ACL1，并将 IPS 配置为内联和故障时开启。此外还包括内部和全局接口上的 IPS。

ASA 配置

```
class-map ips_internalIf
match access-list ACL1

policy-map internalIf
class ips_internalIf
ips inline fail-open

service-policy internalIf interface internalIf
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="ServicePolicy" name="IPS-Policy">
<vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
<vnsAbsFolder key="IPS" name="IPS">
<vnsAbsCfgRel key="TrafficSelection" name="TrafficSelect" targetName="ACL1"/>
<vnsAbsFolder key="IPSSettings" name="IPSSettingsA">
<vnsAbsParam key="operate_mode" name="operate_mode" value="inline"/>
<vnsAbsParam key="fail_mode" name="fail_mode" value="fail-open"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

Sourcefire

此 XML 示例显示处于 fail-open 和仅监控模式下的基本 Sourcefire 配置。

ASA 配置

```
access-list ACL1 extended permit ip any any
class-map sfr_internalIf
match access-list ACL1
policy-map internalIf
class sfr_internalIf
```

```
sfr fail-open monitor-only
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="ACL1">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="Interface" name="internalIf">
<vnsAbsFolder key="ServicePolicy" name="SFR-Policy">
<vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
<vnsAbsFolder key="SFR" name="SFR">
<vnsAbsCfgRel key="TrafficSelection" name="TrafficSelect" targetName="ACL1"/>
<vnsAbsFolder key="SFRSettings" name="SFRSettings">
<vnsAbsParam key="monitor_only" name="operate_mode" value="enable"/>
<vnsAbsParam key="fail_mode" name="fail_mode" value="fail-open"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

网络对象

此 XML 示例设置包含主机 IP 地址和描述的网络对象。

ASA 配置

```
object network ilinux1
host 192.168.1.48
description User1 laptop
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="NetworkObject" name="ilinux1">
<vnsAbsParam key="host_ip_address" name="host_ip_address" value="192.168.1.48"/>
<vnsAbsParam key="description" name="description" value="User1 laptop"/>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
```

```
</fvTenant>
</polUni>
```

网络对象组

此 XML 示例设置包含组名称和组对象的网络对象组。

ASA 配置

```
object-group network Cisco-Network-Object-GroupA
description Cisco inside network
network-object host 192.168.1.51
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="NetworkObjectGroup" name="Cisco-Network-Object-GroupA">
<vnsAbsParam key="description" name="description" value="Cisco inside network"/>
<vnsAbsParam key="host_ip_address" name="host_ip_address" value="192.168.1.51"/>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

高可用性（故障切换）

此 XML 示例启用故障转移，并指定故障转移接口和 IP 地址。

ASA 配置

```
failover
failover lan unit primary
failover lan interface fover GigabitEthernet0/0
failover interface ip fover 192.168.17.1 255.255.255.0 standby 192.168.17.2
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsLIf name="failover_lan">
<vnsRsMetaIf
tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mIfLbl-failover_lan"/>
<vnsRsCIfAtt
tDn="uni/tn-tenant1/lDevVip-Firewall/cDev-ASAP/cIf-[Gig0/0]"/>
</vnsLIf>
```

```
<vnsCDev name="ASAP">
<vnsDevFolder key="FailoverConfig" name="failover_config">
<vnsDevParam key="failover" name="failover" value="enable"/>
<vnsDevParam key="lan_unit" name="lan_unit" value="primary"/>
<vnsDevFolder key="failover_lan_interface" name="failover_lan">
<vnsDevParam key="interface_name" name="interface_name" value="fover"/>
</vnsDevFolder>
<vnsDevFolder key="failover_ip" name="failover_ip">
<vnsDevParam key="interface_name" name="interface_name" value="fover"/>
<vnsDevParam key="active_ip" name="primary_ip" value="192.168.17.1"/>
<vnsDevParam key="netmask" name="netmask" value="255.255.255.0"/>
<vnsDevParam key="standby_ip" name="secondary_ip" value="192.168.17.2"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsCDev>
</vnsLDevVip>
</fvTenant>
</polUni>
```

TCP 服务重置

此 XML 示例为拒绝的入站/出站 TCP 数据包发送重置回复。

ASA 配置

```
service resetinbound | resetoutbount interface interface_name
```

XML 示例

```
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder name="TCPOpt" key="TCPOptions">"
<vnsAbsParam key="inbound_reset" name="reset" value="disable"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

支持 Cisco TrustSec

创建安全对象组

```
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="SecurityObjectGroup" name="coke_sec_obj">
```

```
<vnsAbsParam key="security_group_name" name="sg1" value="mktg"/>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

创建安全组 ACL

```
<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="FROM-OUTSIDE">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
<vnsAbsFolder key="protocol" name="prot1">
<vnsAbsParam key="name_number" name="NN" value="icmp"/>
</vnsAbsFolder>
<vnsAbsFolder key="source_security_group" name="security_group_name">
<vnsAbsParam key="security_group_name" name="security_group_name" value="coke-sec-obj"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>

---------

<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="TEST-ACL">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order10" value="10"/>
<vnsAbsFolder key="protocol" name="protocol">
<vnsAbsParam key="name_number" name="name_number" value="tcp"/>
</vnsAbsFolder>
<vnsAbsFolder key="source_security_group" name="source_security_group">
<vnsAbsCfgRel key="security_object_group" name="security_object_group" targetName="paris"/>
</vnsAbsFolder>
<vnsAbsFolder key="destination_service" name="destination_service">
<vnsAbsParam key="high_port" name="high_port" value="2000"/>
<vnsAbsParam key="low_port" name="low_port" value="800"/>
<vnsAbsParam key="operator" name="operator" value="eq"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni
```

为 TrustSec 配置 AAA 服务器 ISE

```
test1_trustSecxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="TrustSec" name="TrustSec">
<vnsDevFolder key="ISEServerGroup" name="ise">
<vnsDevFolder key="AAAServer" name="ise">
<vnsDevParam key="host" name="host" value="192.168.102.241"/>
<vnsDevParam key="key" name="key" value="cisco123"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
'''
```

将安全组标记 (SGT) 手动分配到 IP 主机映射

```
test2_trustSecxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="TrustSec" name="TrustSec">
<vnsDevFolder key="TrustSecSGTMap" name="SGTMap">
<vnsDevParam key="ip_address" name="ip_address" value="30.30.30.100"/>
<vnsDevParam key="security_group_tag" name="tag" value="100"/>
</vnsDevFolder>
<vnsDevFolder key="TrustSecSGTMap" name="SGTMap2">
<vnsDevParam key="ip_address" name="ip_address" value="2001:3030:30::112"/>
<vnsDevParam key="security_group_tag" name="tag" value="65519"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
'''
```

配置 TrustSec SXP 配置以从 AAA 服务器获取 SGT

```
test3_trustSecxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="TrustSec" name="TrustSec">
<vnsDevFolder key="SXP" name="SXP">
<vnsDevParam key="default_password" name="default_password" value="cisco123"/>
<vnsDevParam key="retry_period" name="retry_period" value="60"/>
<vnsDevParam key="enable" name="enable" value="true"/>
<vnsDevParam key="reconciliation_period" name="reconciliation_period" value="60"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
'''
```

配置 SXP 侦听程序和扬声器

```
test4_trustSecxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="TrustSec" name="TrustSec">
<vnsDevFolder key="SXP" name="SXP">
<vnsDevFolder key="peer" name="peer">
<vnsDevParam key="password" name="password" value="default"/>
<vnsDevParam key="ip_address" name="ip_address" value="192.168.102.240"/>
<vnsDevParam key="mode" name="mode" value="local"/>
<vnsDevParam key="role" name="mode" value="listener"/>
</vnsDevFolder>
<vnsDevFolder key="peer" name="peer2">
<vnsDevParam key="password" name="password" value="default"/>
<vnsDevParam key="ip_address" name="ip_address" value="2001:3030:30::112"/>
<vnsDevParam key="mode" name="mode" value="local"/>
<vnsDevParam key="role" name="mode" value="listener"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
'''
```

访问列表命令的新 remark 关键字

ASA 配置

```
access-list ACL2 remark Remarkable1
access-list ACL2 extended permit tcp any any
access-list ACL2 remark Remarkable2
access-list ACL2 extended permit udp any any
access-list ACL2 remark Remarkable3
access-list ACL2 extended permit icmp any any
```

XML 示例

```
<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="ACL2">
<vnsAbsFolder key="AccessControlEntry" name="ACE2">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
<vnsAbsParam key="remark" name="remark1" value="Remarkable1"/>
<vnsAbsFolder key="protocol" name="protocol1">
<vnsAbsParam key="name_number" name="pNN1" value="tcp"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="AccessControlEntry" name="ACE3">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order3" value="3"/>
<vnsAbsParam key="remark" name="remark2" value="Remarkable2"/>
```

```
<vnsAbsFolder key="protocol" name="protocol3">
<vnsAbsParam key="name_number" name="pNN3" value="udp"/>
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="AccessControlEntry" name="ACE4">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order4" value="4"/>
<vnsAbsParam key="remark" name="remark3" value="Remarkable3"/>
<vnsAbsFolder key="protocol" name="protocol4">
<vnsAbsParam key="name_number" name="pNN4" value="icmp"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

全局应用检测

ASA 配置

```
policy-map global_policy
class inspection_default
inspect rsh
inspect dns preset_dns_map
inspect rtsp
inspect h323 h225
inspect skinny
inspect sip
inspect ip-options
inspect xdmcp
inspect sunrpc
inspect sqlnet
inspect tftp
inspect h323 ras
inspect esmtp
inspect netbios
inspect ftp
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="GlobalServicePolicy" name="GlobalServicePolicy">
<vnsDevParam key="ServicePolicyState" name="ServicePolicyState" value="enable"/>
<vnsDevFolder key="ApplicationInspection" name="ApplicationInspection">
<vnsDevFolder key="InspectionSettings" name="InspectionSettings">
<vnsDevParam key="tftp" name="tftp" value="enable"/>
<vnsDevParam key="rtsp" name="rtsp" value="enable"/>
<vnsDevParam key="h323_h225" name="h323_h225" value="enable"/>
<vnsDevParam key="skinny" name="skinny" value="enable"/>
<vnsDevParam key="sip" name="sip" value="enable"/>
<vnsDevParam key="esmtp" name="esmtp" value="enable"/>
<vnsDevParam key="ftp" name="ftp" value="enable"/>
<vnsDevParam key="h323_ras" name="h323_ras" value="enable"/>
```

```
<vnsDevParam key="sunrpc" name="sunrpc" value="enable"/>
<vnsDevParam key="ip_options" name="ip_options" value="enable"/>
<vnsDevParam key="xdmcp" name="xdmcp" value="enable"/>
<vnsDevParam key="sqlnet" name="sqlnet" value="enable"/>
<vnsDevParam key="dns_preset" name="dns_preset" value="enable"/>
<vnsDevParam key="netbios" name="netbios" value="enable"/>
<vnsDevParam key="rsh" name="rsh" value="enable"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

新 same-security-traffic 命令

ASA 配置

```
Same-security-traffic permit inter-interface
Same-security-traffic permit intra-interface
```

XML 示例

```
<polUni>
<fvTenant name="tenant1">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="SameSecurityTraffic" name="SameSecurityTraffic">
<vnsDevParam key="inter_interface" name="inter_interface" value="permit"/>
<vnsDevParam key="intra_interface" name="intra_interface" value="permit"/>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

新 time-range 命令

ASA 配置

```
time-range T1-time-range
absolute start 08:09 07 August 2016 end 12:20 23 September 2018
periodic Tuesday Thursday 8:09 to 20:00
periodic Wednesday 5:07 to Tuesday 17:00

access-list example-list extended permit ip any any time-range T1-time-range
```

XML 示例

```
<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
```

```
<vnsAbsFolder key="TimeRange" name="T1-time-range">
<vnsAbsFolder key="AbsoluteTimeDate" name="AbsoluteTimeDate">
<vnsAbsFolder key="End" name="End">
<vnsAbsParam key="year" name="year" value="2016" />
<vnsAbsParam key="day" name="day" value="23" />
<vnsAbsParam key="month" name="month" value="09" />
<vnsAbsParam key="time" name="time" value="12:20" />
</vnsAbsFolder>
<vnsAbsFolder key="Start" name="Start">
<vnsAbsParam key="year" name="year2" value="2014" />
<vnsAbsParam key="day" name="day" value="07" />
<vnsAbsParam key="month" name="month" value="8" />
<vnsAbsParam key="time" name="time" value="8:9" />
</vnsAbsFolder>
</vnsAbsFolder>
<vnsAbsFolder key="WeeklyPeriod" name="WeeklyPeriod">
<vnsAbsParam key="start_day" name="start_day" value="Wednesday" />
<vnsAbsParam key="end_day" name="end_day" value="Tuesday" />
<vnsAbsParam key="start_time" name="start_time" value="5:7" />
<vnsAbsParam key="end_time" name="end_time" value="17:00" />
</vnsAbsFolder>
<vnsAbsFolder key="DailyPeriod" name="DailyPeriod">
<vnsAbsParam key="day" name="day" value="Tuesday Thursday" />
<vnsAbsParam key="start_time" name="start_time" value="8:9" />
<vnsAbsParam key="end_time" name="end_time" value="20:00" />
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

站点间 VPN 配置

ASA 配置

```
access-list ACL1 extended permit ip any any
crypto ipsec ikev2 ipsec-proposal ASA-DP
 protocol esp encryption aes-gcm-256 aes-gcm-192 aes-256 aes-192 aes 3des aes-gmac-256 aes-gmac-192
 protocol esp integrity sha-512 sha-384 sha-256 sha-1 null
crypto map externalIf 1 match address ACL1
crypto map externalIf 1 set pfs group14
crypto map externalIf 1 set peer 10.5.1.101
crypto map externalIf 1 set ikev2 ipsec-proposal ASA-DP
crypto map externalIf 1 set security-association lifetime seconds 120
crypto map externalIf 1 set security-association lifetime kilobytes 120
crypto ikev2 policy 10
 encryption aes-256 aes-192 aes 3des
 integrity sha512 sha384 sha256 sha
 group 21 20 19 24 14 5 2 1
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 21 20 19 24 14 5 2 1
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
crypto ikev2 enable externalIf
```

```
group-policy externalIf_10.5.1.101 internal
group-policy externalIf_10.5.1.101 attributes
 vpn-tunnel-protocol ikev2
tunnel-group 10.5.1.101 type ipsec-l2l
tunnel-group 10.5.1.101 general-attributes
 default-group-policy externalIf_10.5.1.101
tunnel-group 10.5.1.101 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco1234
 ikev2 local-authentication pre-shared-key cisco123
```

XML 示例

```
testACLxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="AccessList" name="ACL1">
<vnsAbsFolder key="AccessControlEntry" name="ACE1">
<vnsAbsParam key="action" name="action1" value="permit"/>
<vnsAbsParam key="order" name="order1" value="1"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
'''
testS2SVPNxml='''\
<polUni>
<fvTenant name="tenant1">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
<vnsAbsDevCfg>
<vnsAbsFolder key="Interface" name="externalIf">
<vnsAbsFolder key="S2SVPNPolicy" name="S2SVPNPolicy">
<vnsAbsParam key="peer_ip" name="peer_ip" value="10.5.1.101"/>
<vnsAbsParam key="pre_shared_key_local" name="pre_shared_key_local" value="cisco123"/>
<vnsAbsParam key="pre_shared_key_remote" name="pre_shared_key_remote" value="cisco1234"/>
<vnsAbsParam key="order" name="order" value="1"/>
<vnsAbsCfgRel key="traffic_selection" name="traffic_selection" targetName="ACL1"/>
<vnsAbsFolder key="Advanced" name="Advanced">
<vnsAbsParam key="pfs" name="pfs" value="group14"/>
<vnsAbsParam key="sa_lifet_time_in_seconds" name="life_sec" value="120"/>
<vnsAbsParam key="sa_lifet_time_in_kilobytes" name="life_kb" value="120"/>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsFolder>
</vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
'''
```

接口说明

ASA 配置

```
interface GigabitEthernet0/0.306
 description internet access interface
 vlan 306
 nameif externalIf
 security-level 50
 ip address 20.0.0.1 255.255.255.0
!
```

XML 示例

```
<vnsFolderInst cardinality="unspecified" ctrctNameOrLbl="C1" devCtxLbl="" graphNameOrLbl="GRAPH1"
  key="InterfaceConfig" locked="no" name="externalIfCfg" nameAlias="" nodeNameOrLbl="N1" scopedBy="epg">
 <vnsParamInst cardinality="unspecified" key="description" locked="no" mandatory="no" name="description"
   nameAlias="" validation="" value="internet access interface" />
 <vnsParamInst cardinality="unspecified" key="security_level" locked="no" mandatory="no"
name="external_security_level"
   nameAlias="" validation="" value="50" />
 <vnsFolderInst cardinality="unspecified" ctrctNameOrLbl="C1" devCtxLbl="" graphNameOrLbl="GRAPH1"
   key="IPv4Address" locked="no" name="IPv4Address" nameAlias="" nodeNameOrLbl="N1" scopedBy="epg">
  <vnsParamInst cardinality="unspecified" key="ipv4_address" locked="no" mandatory="no" name="ipv4_address"
    nameAlias="" validation="" value="20.0.0.1/24" />
 </vnsFolderInst>
</vnsFolderInst>
```

当日消息

ASA 配置

```
banner motd Have a nice day!
```

XML 示例

```
testMOTDxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="Banner" name="Banner">
                <vnsDevParam key="motd" name="motd" value="Have a nice day!"/>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

恢复配置

XML 示例

```
<vnsMFunc name="Firewall">
<vnsMFolder key="ExIntfConfigRelFolder"
  dispLabel="External Interface Configuration"
  description="A list of additional interface parameters for external connector"...>
<vnsMFolder key="InIntfConfigRelFolder"
  dispLabel="Internal Interface Configuration"
  description="A list of additional interface parameters for internal connector"...>
 <vnsMConn name="external" ...>
 <vnsMConn name="internal" ...>
 <vnsMFolder key="SecurityPolicyAssignment"
   dispLabel="Security Policy Assignment"
   description="Assign the security policy in the named file to the service-graph">
  <vnsMParam key="ConfigFile"
    dispLabel="Configuration File"
    dType="str"
    description="Specify the name of the file that contains the out of band configuration specific to the
service-graph"/>
 </vnsMFolder>
</vnsMFunc>
```

SNMPv3 配置

使用集群参数的 SNMPv3 配置：

ASA 配置

```
snmp-server group SNMPv3UserGroup v3 priv
snmp-server user user1 SNMPv3UserGroup v3 engineID 80000009fe402281327058539814e8658211c04ef63ef71e5a encrypted
 auth md5 a5:f1:ce:24:cc:57:1e:fd:51:1d:e3:e3:39:0f:bd:f9 priv aes 128
a5:f1:ce:24:cc:57:1e:fd:51:1d:e3:e3:39:0f:bd:f9
snmp-server host management 1.1.1.1 poll version 3 user1
snmp-server location SJC
snmp-server contact admin@company.com
```

XML 示例

```
testSNMPclusterxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="SNMP" name="SNMP">
                    <vnsDevParam key="location" name="location" value="SJC"/>
                    <vnsDevParam key="contact" name="contact" value="admin@company.com"/>
                <vnsDevFolder key="User" name="user1">
                    <vnsDevParam key="PrivacyPassword" name="PrivacyPassword" value="uall"/>
                    <vnsDevParam key="AuthenticationPassword" name="AuthenticationPassword" value="authuall"/>

                    <vnsDevParam key="AesSize" name="AesSize" value="128"/>
                </vnsDevFolder>
                <vnsDevFolder key="Host" name="Host">
                    <vnsDevParam key="IP" name="IP" value="1.1.1.1"/>
                    <vnsDevParam key="interface" name="interface" value="management"/>
                    <vnsDevParam key="user" name="user" value="user1"/>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

使用服务参数的 SNMPv3 配置：

首先，使用集群参数配置用户：

ASA 配置

```
snmp-server user user2 SNMPv3UserGroup v3 engineID 80000009fe402281327058539814e8658211c04ef63ef71e5a encrypted
 auth md5 a5:f1:ce:24:cc:57:1e:fd:51:1d:e3:e3:39:0f:bd:f9 priv aes 256
a5:f1:ce:24:cc:57:1e:fd:51:1d:e3:e3:39:0f:bd:f9
```

XML 示例

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="SNMP" name="SNMP">
                <vnsDevFolder key="User" name="user2">
                    <vnsDevParam key="PrivacyPassword" name="PrivacyPassword" value="uall2"/>
                   <vnsDevParam key="AuthenticationPassword" name="AuthenticationPassword" value="authuall2"/>

                    <vnsDevParam key="AesSize" name="AesSize" value="256"/>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

然后，使用服务参数配置服务器：

ASA 配置

```
snmp-server host internalIf 30.30.30.70 poll version 3 user2
```

XML 示例

```
testSNMPservicexml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Interface" name="internalIf">
                        <vnsAbsFolder name="SNMPHost" key="SNMPHost">
                            <vnsAbsParam key="IP" name="ip" value="30.30.30.70"/>
                            <vnsAbsParam key="user" name="user" value="user1"/>
                        </vnsAbsFolder>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
```

```
          </vnsAbsGraph>
    </fvTenant>
</polUni>
'''
```

集群设置

此 XML 示例启用集群并指定集群接口和 IP 地址：

ASA 配置

```
ip local pool __$MAN_ADDRESS_POOL_IPV4$_ 192.168.102.161-192.168.102.162 mask 255.255.255.0
interface Management0/0
 ip address 192.168.102.160 255.255.255.0 cluster-pool __$MAN_ADDRESS_POOL_IPV4$_
!
interface GigabitEthernet0/3
 description Clustering Interface
!
cluster interface-mode spanned
cluster group ClusterConfig
 key *****
 local-unit clusterMasterINDrouted
 cluster-interface GigabitEthernet0/3 ip 7.7.7.160 255.255.255.0
 priority 1
 health-check holdtime 3
 health-check data-interface auto-rejoin 3 5 2
 health-check cluster-interface auto-rejoin unlimited 5 1
 health-check system auto-rejoin 3 5 2
 health-check monitor-interface debounce-time 9000
 clacp system-mac auto system-priority 1
 enable
```

XML 示例

首先，将集群中的所有 ASA 单元注册为 LDev（逻辑设备）下的 CDevs（具体设备）：

```
<polUni>
    <fvTenant name="tenantClusterSpannedRouted">
            <vnsLDevVip name="Firewall">
                            <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.3"/>
                            <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
                            <vnsCMgmt host="192.168.102.160" port="443" subnetmask="0.0.0.0"/>
                                <vnsCCred name="username"  value="management-user"/>
                                <vnsCCredSecret name="password" value="cisco"/>
                                <vnsCDev name="clusterMasterINDrouted">
                                    <vnsCMgmt gateway="0.0.0.0" host="192.168.102.160" port="443"/>
                                    <vnsCIf name="Port-channel2">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/6]"/>
                                    </vnsCIf>
                                    <vnsCIf name="GigabitEthernet0/3">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/7]"/>
                                    </vnsCIf>
                                    <vnsCIf name="Port-channel1">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/5]"/>
                                    </vnsCIf>
                                    <vnsCCredSecret name="password" value="cisco"/>
                                    <vnsCCred name="username" value="management-user"/>
                                </vnsCDev>
                                <vnsCDev name="clusterSlaveINDrouted">
                                    <vnsCMgmt gateway="0.0.0.0" host="192.168.102.162" port="443"/>
                                    <vnsCIf name="Port-channel2">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/9]"/>
                                    </vnsCIf>
                                    <vnsCIf name="GigabitEthernet0/3">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/10]"/>
                                    </vnsCIf>
                                    <vnsCIf name="Port-channel1">
                                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/8]"/>
                                    </vnsCIf>
                                    <vnsCCredSecret name="password" value="cisco"/>
                                    <vnsCCred name="username" value="management-user"/>
                                 </vnsCDev>
                                 <vnsLIf name="inside">
                                 <vnsRsMetaIf tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-internal"/>
                                     <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterMasterINDrouted/cIf-[Port-channel2]"/>
                                     <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterSlaveINDrouted/cIf-[Port-channel2]"/>
                                  </vnsLIf>
                                  <vnsLIf name="outside">
                                  <vnsRsMetaIf tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-external"/>
                                      <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterMasterINDrouted/cIf-[Port-channel1]"/>
                                      <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterSlaveINDrouted/cIf-[Port-channel1]"/>
                                  </vnsLIf>
                                  <vnsLIf name="cluster_ctrl_lk">
                                  <vnsRsMetaIf tDn="uni/infra/mDev-CISCO-ASA-1.3/mIfLbl-cluster_ctrl_lk"/>
                                      <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterSlaveINDrouted/cIf-[GigabitEthernet0/3]"/>

                                      <vnsRsCIfAttN
tDn="uni/tn-tenantClusterSpannedRouted/lDevVip-Firewall/cDev-clusterMasterINDrouted/cIf-[GigabitEthernet0/3]"/>

                                  </vnsLIf>
            </vnsLDevVip>
    </fvTenant>
</polUni>
```

然后，配置集群配置：

```
<polUni>
<fvTenant name="tenantClusterSpannedRouted">
<vnsLDevVip name="Firewall">
<vnsDevFolder key="ClusterConfig" name="ClusterConfig">
<vnsDevParam key="apic_managed" name="apic_managed" value="enable"/>
<vnsDevFolder key="Bootstrap" name="Bootstrap">
<vnsDevParam key="key" name="key" value="cisco123"/>
<vnsDevParam key="interface_mode" name="interface_mode" value="spanned"/>
<vnsDevParam key="ctrl_intf" name="ctrl_intf" value="gigabitEthernet0/3"/>
<vnsDevParam key="ctrl_intf_address" name="ctrl_intf_address" value="7.7.7.7/24"/>
</vnsDevFolder>
</vnsDevFolder>
</vnsLDevVip>
</fvTenant>
</polUni>
```

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。